NETFOUNDRY™
SPIN UP YOUR NETWORK

SECURITY PAPER

How Do Ransomware Actors Scope Opportunities?

How Ransomware actors scope opportunities?

In part 1 of this series, I discussed various tactics and techniques malicious actors use to find and attack their targets. In this paper, I discuss how relatively simple and automated it is for bad actors to source specific details about internet facing infrastructure, that can be used as potential exploit targets, and much of these details are available from publicly (free) available sources. All three papers are available from the NetFoundry web site.

Before showing how simple it can be to take some of these steps yourself, I want to point out how much information is in the public domain. These days, most ransomware victims are targets of opportunity. The automated attack techniques discussed in this series may find and exploit soft spots. These attacks may or may not be targeted, and they may be motivated by profit (e.g. ransomware), disrupting operations (e.g. denial of service) IP theft, or espionage.

Common starting points for finding information to aid in targeting

IP addresses, those strings of digits separated by 's for IPv4 and :'s for IPv6, are difficult for non-technical users to grasp. Most users prefer to use the symbolic domain names like cnn.com, microsoft.com, or netfoundry.io. However, IP addresses may be easily investigated by an attacker in a reverse look up database to reveal useful facts that they may be able to leverage in an attack.

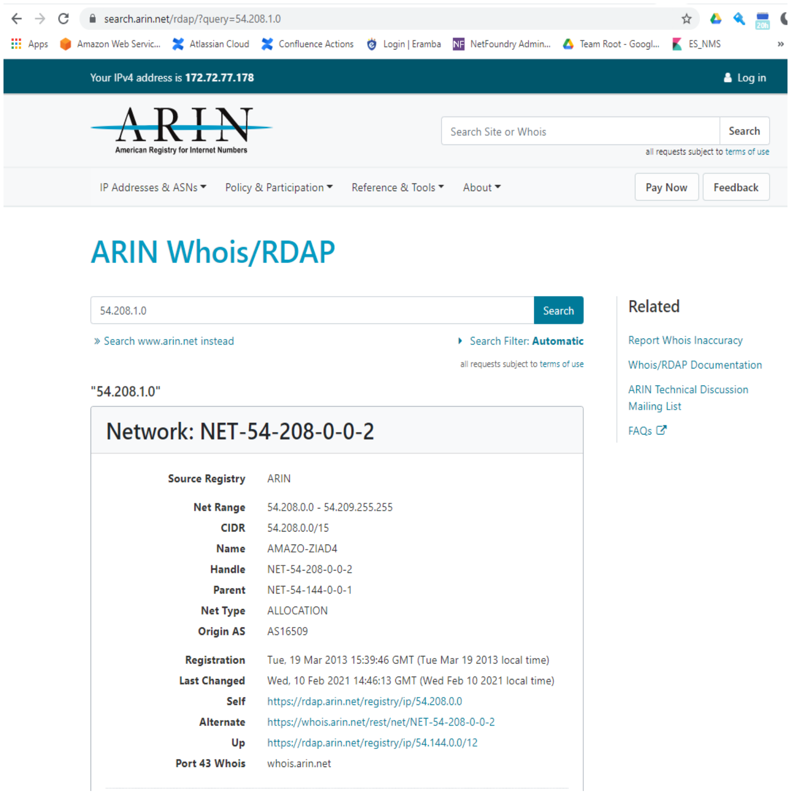
One of the oldest and simplest tools is a command line or website service called whois. It even has its own specific technique designation in the MITRE ATT&CK® Framework (T1596.002). If you have a single IP address in a range you can look up the owner(s) and find out the total size of the range, among other things. Similarly, domain names can be investigated to reveal for ownership and contact information. This can be very useful in targeted attacks, where a bad actor seeks to find the scope of a target's network resources. Whois can be run from a command line or by visiting https://whois.com.

Here is an example of the whois command in a Linux shell. Note there are clues here about the geography and identity of the responsible party.

```
user@system:~$ whois 208.31.160.18
…
NetRange:    208.0.0.0 - 208.35.255.255
CIDR:        208.0.0.0/11, 208.32.0.0/14
NetName:     SPRINTLINK-BLKS
NetHandle:   NET-208-0-0-0-1
Parent:      NET208 (NET-208-0-0-0-0)
NetType:     Direct Allocation
OriginAS:
Organization:   Sprint (SPRN-Z)
RegDate:     1996-03-13
Updated:     2020-12-29
Comment:     ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
Ref:         https://rdap.arin.net/registry/ip/208.0.0.0
OrgName:     Sprint
OrgId:       SPRN-Z
 …
CIDR:        208.31.160.0/24
NetName:     SPRINTLINK
NetHandle:   NET-208-1-158-0-1
Parent:      SPRINTLINK-BLKS (NET-208-0-0-0-1)
…
OrgName:     Company Inc
```

OrgId: Com-1

```
Address:     12 Street Ave
City:        Hometown
StateProv:   NY
PostalCode:  01010
Country:     US
RegDate:     1995-04-13
Updated:     2011-09-24
Comment:     Company Inc IP Network
```



Your IPv4 address is **172.72.77.178**

ARIN Whois/RDAP

54.208.1.0

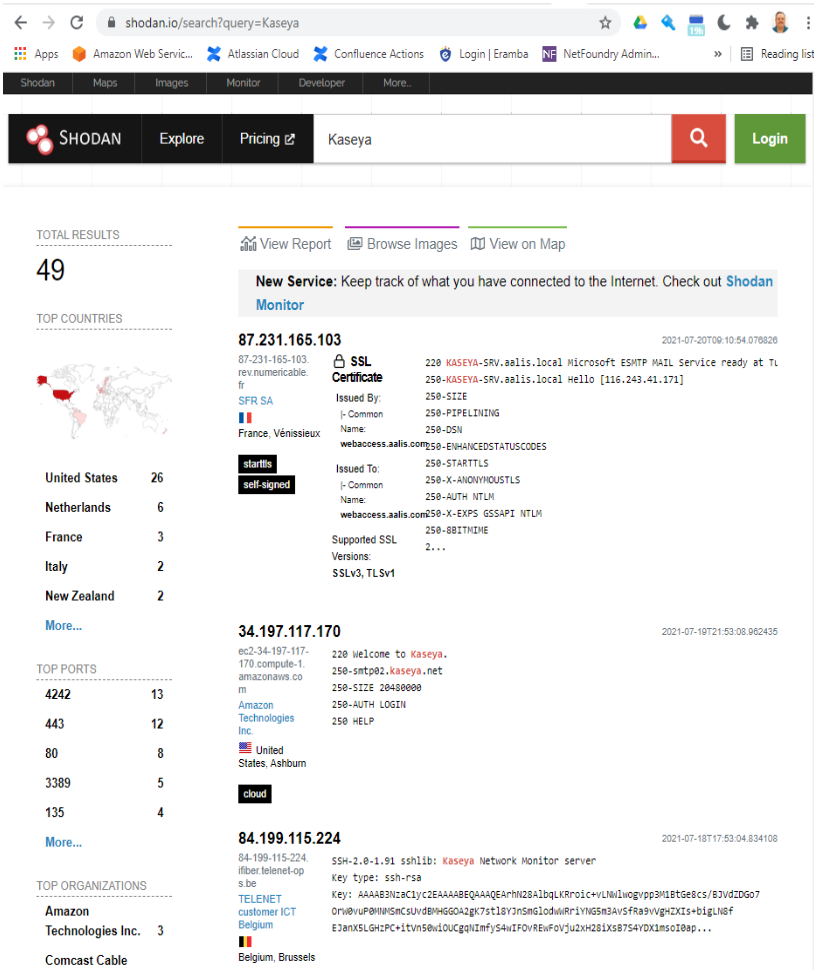
"54.208.1.0"

Network: NET-54-208-0-0-2

Source Registry	ARIN
Net Range	54.208.0.0 - 54.209.255.255
CIDR	54.208.0.0/15
Name	AMAZO-ZIAD4
Handle	NET-54-208-0-0-2
Parent	NET-54-144-0-0-1
Net Type	ALLOCATION
Origin AS	AS16509
Registration	Tue, 19 Mar 2013 15:39:46 GMT (Tue Mar 19 2013 local time)
Last Changed	Wed, 10 Feb 2021 14:46:13 GMT (Wed Feb 10 2021 local time)
Self	https://rdap.arin.net/registry/ip/54.208.0.0
Alternate	https://whois.arin.net/rest/net/NET-54-208-0-0-2
Up	https://rdap.arin.net/registry/ip/54.144.0.0/12
Port 43 Whois	whois.arin.net

Another very popular public source of information regarding networks, ports, and their related services is Shodan. This security research tool is constantly scanning the internet to create a database of all responding IP addresses, IP ports, and details about the applications responding on the port. For example, SSL server certificates, protocol greeting and banner messages identifying the application version or operating system or both.

Shodan is free for casual research without a login, and additional query features are available for account holders. The recent Kaseya ransomware attack had many users looking up the targets in Shodan. Incredibly, there are still Kaseya nodes responding on the internet, though they may not be the same vulnerable KSA servers that were targeted. One reporter noted that the day of the attack, more than 1000 such servers were visible. As I write this the count is down to 49 as word of the vulnerabilities spread among users of the affected application.



TOTAL RESULTS

49

TOP COUNTRIES

United States	26
Netherlands	6
France	3
Italy	2
New Zealand	2
More...	

TOP PORTS

4242	13
443	12
80	8
3389	5
135	4
More...	

TOP ORGANIZATIONS

Amazon Technologies Inc.	3
Comcast Cable	

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

87.231.165.103 2021-07-20T09:10:54.076826

87-231-165-103.rev.numericable.fr
SFR SA
France, Vénissieux
starttls
self-signed

SSL Certificate
Issued By:
|- Common Name: **webaccess.aalis.com**
Issued To:
|- Common Name: **webaccess.aalis.com**
Supported SSL Versions: **SSLv3, TLSv1**

```
220 KASEYA-SRV.aalis.local Microsoft ESMTP MAIL Service ready at Tu
250-KASEYA-SRV.aalis.local Hello [116.243.41.171]
250-SIZE
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-X-ANONYMOUSTLS
250-AUTH NTLM
250-X-EXPS GSSAPI NTLM
250-8BITMIME
2...
```

34.197.117.170 2021-07-19T21:53:08.962435

ec2-34-197-117-170.compute-1.amazonaws.com
Amazon Technologies Inc.
United States, Ashburn
cloud

```
220 Welcome to Kaseya.
250-smtp02.kaseya.net
250-SIZE 20480000
250-AUTH LOGIN
250 HELP
```

84.199.115.224 2021-07-18T17:53:04.834108

84-199-115-224.ifiber.telenet-ops.be
TELENET customer ICT Belgium
Belgium, Brussels

```
SSH-2.0-1.91 sshlib: Kaseya Network Monitor server
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAABEQAAAQEArhN28AlbqLKRroic+vLNWlwogvpp3M1BtGe8cs/BJVdZDGo7
OrW0vuP0MNMSmCsUvdBMHGGOA2gK7stl8YJnSmGlodwWRriYNG5m3AvSfRa9vVgHZXIs+bigLN8f
EJanX5LGHzPC+itVn50wiOUCgqNImfyS4wIFOvREwFoVju2xH28iXsB7S4YDX1msoI0ap...
```

Anyone and anything connected to the internet is at risk.

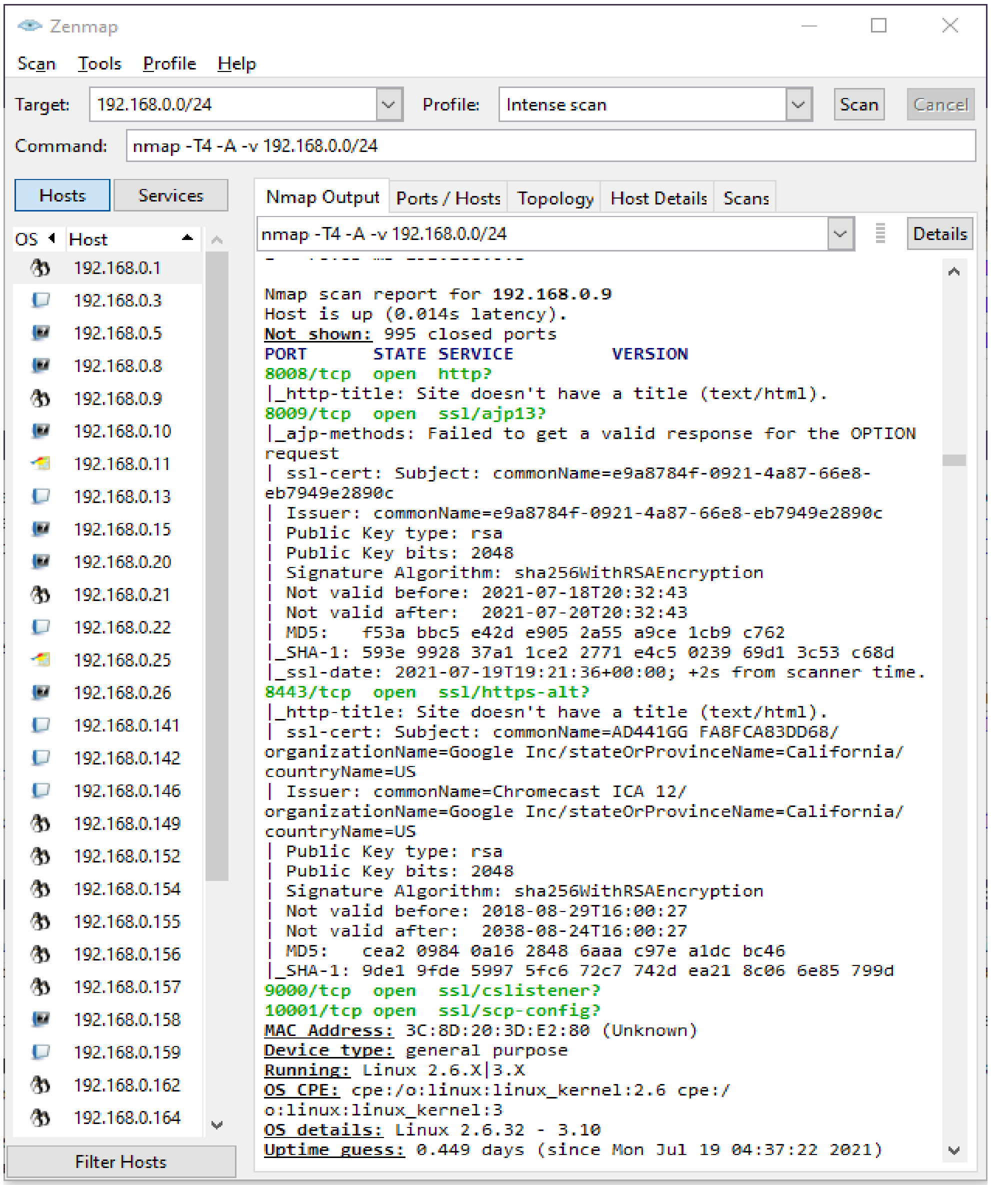
I am bringing this information forward in part to illustrate how simple it is to find detailed information about internet facing infrastructure, and to also help dispel the myth that only high-value targets or popular companies are vulnerable. The reality is, if your organization has ANY internet facing infrastructure that allows incoming traffic from the Internet – you are a potential target.

There are two main drivers in the hacking world today; espionage, and pure criminal profit. The majority is, sadly, criminal. There are some 2200 cyberattacks per day and ransoms continue to increase. So, how specifically do these malicious actors find their targets in the wide world if they are looking for a particular vulnerability to exploit? We've noted some techniques above, but there are more active methods in general use.

As noted in the part one of this series, Active Scanning (T1595) is commonly used to find potential targets. I will discuss both IP Block Scanning (T1595.001) and Vulnerability Scanning (T1595.002), and some freely available tools that anyone can use to emulate the hacker's work.

IP Block Scanning is a very useful technique. I've used it many times personally to find the addresses of various devices attached to my wireless network to access them directly, or to configure something. The elder statesman of IP address scanning is Nmap. Nmap was first released in Phrack magazine in 1997 as source code. It has been in constant development since then and is extremely compact, efficient, and easy to use.

There are many graphical interfaces for NmaP, such as Zenmap, shown below. To use the tool, one must only start the software, plug in an address or subnet, and hit "Scan". The actual scanning command is created for you, and the scanning begins. The image below is of a scan of a private network, and the specific device is a Chromecast. You can see the noted open ports and certificate information which provides clues as to what the device is and who manufactured it. This seemingly basic information could provide key clues if one wanted to attack the device.



Target: 192.168.0.0/24

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.0.0/24

```
OS  Host
    192.168.0.1
    192.168.0.3
    192.168.0.5
    192.168.0.8
    192.168.0.9
    192.168.0.10
    192.168.0.11
    192.168.0.13
    192.168.0.15
    192.168.0.20
    192.168.0.21
    192.168.0.22
    192.168.0.25
    192.168.0.26
    192.168.0.141
    192.168.0.142
    192.168.0.146
    192.168.0.149
    192.168.0.152
    192.168.0.154
    192.168.0.155
    192.168.0.156
    192.168.0.157
    192.168.0.158
    192.168.0.159
    192.168.0.162
    192.168.0.164
```

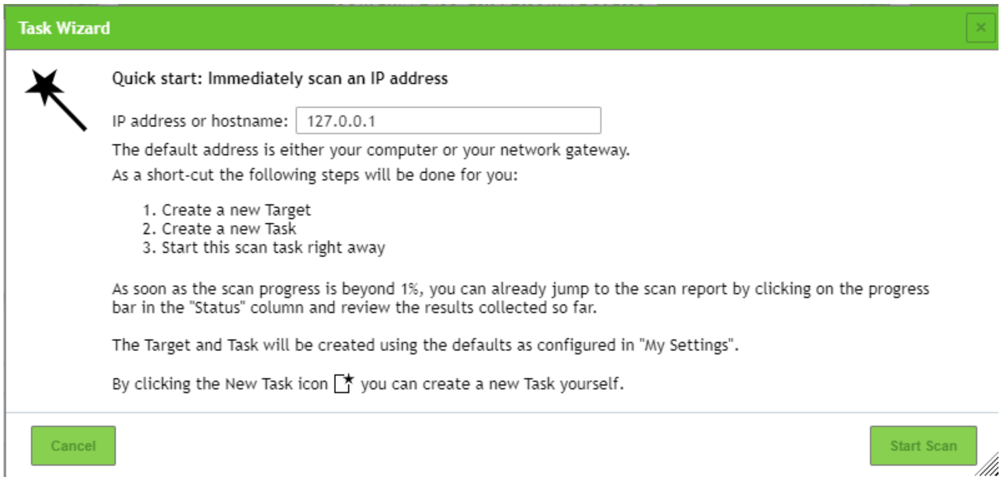
```
nmap -T4 -A -v 192.168.0.0/24

Nmap scan report for 192.168.0.9
Host is up (0.014s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE         VERSION
8008/tcp  open  http?
|_http-title: Site doesn't have a title (text/html).
8009/tcp  open  ssl/ajp13?
|_ajp-methods: Failed to get a valid response for the OPTION
request
| ssl-cert: Subject: commonName=e9a8784f-0921-4a87-66e8-
eb7949e2890c
| Issuer: commonName=e9a8784f-0921-4a87-66e8-eb7949e2890c
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-07-18T20:32:43
| Not valid after:  2021-07-20T20:32:43
| MD5:   f53a bbc5 e42d e905 2a55 a9ce 1cb9 c762
|_SHA-1: 593e 9928 37a1 1ce2 2771 e4c5 0239 69d1 3c53 c68d
|_ssl-date: 2021-07-19T19:21:36+00:00; +2s from scanner time.
8443/tcp  open  ssl/https-alt?
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=AD441GG FA8FCA83DD68/
organizationName=Google Inc/stateOrProvinceName=California/
countryName=US
| Issuer: commonName=Chromecast ICA 12/
organizationName=Google Inc/stateOrProvinceName=California/
countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2018-08-29T16:00:27
| Not valid after:  2038-08-24T16:00:27
| MD5:   cea2 0984 0a16 2848 6aaa c97e a1dc bc46
|_SHA-1: 9de1 9fde 5997 5fc6 72c7 742d ea21 8c06 6e85 799d
9000/tcp  open  ssl/cslistener?
10001/tcp open  ssl/scp-config?
MAC Address: 3C:8D:20:3D:E2:80 (Unknown)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/
o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Uptime guess: 0.449 days (since Mon Jul 19 04:37:22 2021)
```

The scan shown above took a few minutes to execute against a 256 address subnet. Of course, all of this can be scripted, and additional automation performed with the resulting data by even a beginning programmer.

The next technique in Active Scanning is Vulnerability Scanning (T1595.002). Vulnerability scanning is a bit more complicated than IP scanning, but not that much. A popular tool is Greenbone Security Assistant, formerly OpenVAS.

Vulnerability scanning runs tests against ports to elicit responses that indicate a node is subject to a vulnerability. These tests may indicate the node is potentially vulnerable in that it may certain versions that have bugs that are exploitable, or general services are subject to crashes when passed bad data. There are tens of thousands of possible vulnerabilities that can be checked. Responsible network administrators and security teams perform these kinds of checks against their own systems regularly to discover and mitigate any flaws before attackers can. However, many, many internet-connected devices are vulnerable, as proven by the increasing successful ransomware attacks.

Larger and more complicated than an IP scanner, Greenbone is delivered as a virtual machine image, rather than a set of executable files. Greenbone has a wizard, which most users of software are familiar with, to make the running of the scanner simple. Pick a target (perhaps from your Nmap scan), and press "Start Scan".



Quick start: Immediately scan an IP address

IP address or hostname: 127.0.0.1

The default address is either your computer or your network gateway.
As a short-cut the following steps will be done for you:

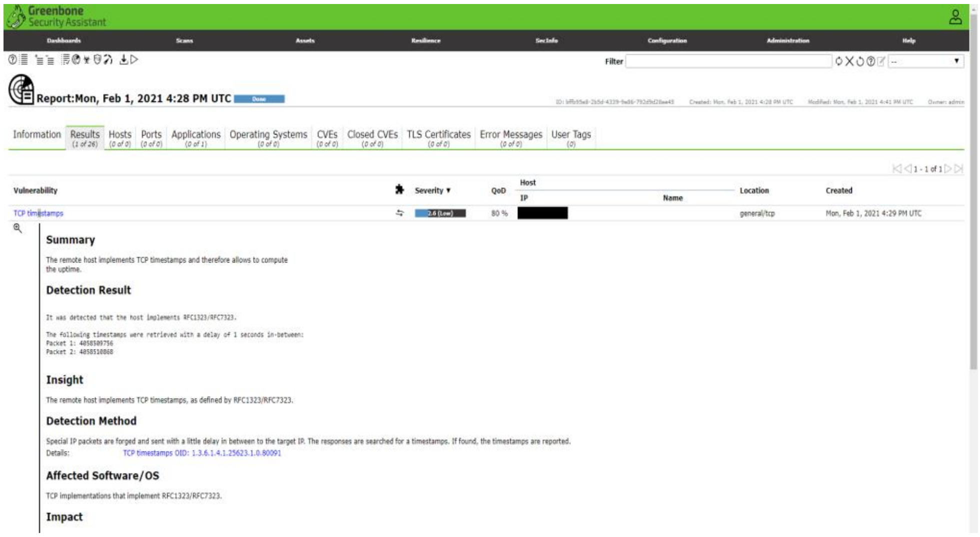
1. Create a new Target
2. Create a new Task
3. Start this scan task right away

As soon as the scan progress is beyond 1%, you can already jump to the scan report by clicking on the progress bar in the "Status" column and review the results collected so far.

The Target and Task will be created using the defaults as configured in "My Settings".

By clicking the New Task icon you can create a new Task yourself.

When complete, the report will include information such as that below. This vulnerability is common, and mostly innocuous, but shows us the kind of information provided by Greenbone or other vulnerability scanners. We can see the host (blacked out here), port, vulnerability description, and other information. Additionally, there are mitigation steps available. For the defender, this is a wealth of information to utilize in their own defense. For the attacker, this is a detailed map into your organization.



Report:Mon, Feb 1, 2021 4:28 PM UTC Done

ID: bffb55e8-2b5d-4339-9e86-792d9d28ee45 Created: Mon, Feb 1, 2021 4:28 PM UTC Modified: Mon, Feb 1, 2021 4:41 PM UTC Owner: admin

Information | Results (1 of 26) | Hosts (0 of 0) | Ports (0 of 0) | Applications (0 of 1) | Operating Systems (0 of 0) | CVEs (0 of 0) | Closed CVEs (0 of 0) | TLS Certificates (0 of 0) | Error Messages (0 of 0) | User Tags (0)

1 - 1 of 1

Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
TCP timestamps	⇆	2.6 (Low)	80 %	[redacted]		general/tcp	Mon, Feb 1, 2021 4:29 PM UTC

Summary

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Detection Result

```
It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 4058509756
Packet 2: 4058510868
```

Insight

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: TCP timestamps OID: 1.3.6.1.4.1.25623.1.0.80091

Affected Software/OS

TCP implementations that implement RFC1323/RFC7323.

Impact

Exploiting vulnerabilities

Once potential targets have been located, malicious actors have a few ways they may use to take a next step. Potential exploits discovered by vulnerability scanning can be leveraged using various tool sets available for the purpose. Metasploit is one of the oldest and best known, making some exploits terribly simple to execute. Another very common technique is Credential Stuffing (T1110.004).

Once successful at gaining access, the attacker will often take the opportunity to collect user credentials, usernames, and passwords. These credentials can be used to continue to explore network and organization assets to gain access additional services, resources, and information. Further, these compromised credentials may be hugely valuable, and can be sold, bartered and exchanged on the dark web to other interested parties. By combining and selling these credentials, hackers continue to monetize their work, and assist other attacks.

Unfortunately, users, no matter how often they are told not to, do reuse passwords. Since many email addresses are variations on a name, and various databases collect emails, user names, and passwords, attackers can use the captured lists to target new systems. The Colonial Pipeline hack may have been aided by this technique. With name comparison, and perhaps targeting using information collected via LinkedIn or other sources, this kind of attack technique can greatly increase the chances of an attacker gaining access via a Valid Account (T1078) to External Remote Services (T1133), such as a VPN or Remote Desktop.

Recently, Combination of Many Breaches (COMB) has appeared as a new threat. The Combination of Many Breaches is a huge database of credentials distributed with tools to query and extract information easily. We won't discuss how to gather this sort of information, as that is a dangerous game, but there are many security companies and sites that do and make the data available for individual users.

Any of the following links contain multiple collections of credentials. I urge you to search your own email addresses to find if you exist in any of those collections. If you do, understand that this does not mean someone has the credentials to your email account, but some site which identified you with email was hacked, and the passwords dumped. This could be your email provider; it could be your favorite delivery service or favorite restaurant that offers online ordering. There is no way to tell. However, finding out you have been compromised at all should serve as a reminder not to reuse passwords.

https://haveibeenpwned.com/
https://cybernews.com/personal-data-leak-check/
https://sec.hpi.de/ilc/search

I hope that the information above has helped you understand that the common notion that there are determined sophisticated teams of hacker working in the dark to take down specific targets for a big payday is often a false one. Unfortunately, malware/ransomware is primarily a criminal enterprise actively working to pick off the lowest hanging fruit. The actual work is largely automated, relatively simple, and ongoing every hour of every day.

Ransomware is big business, getting bigger, and will continue to be until it is no longer profitable. Everyone and every business should take the threat seriously, and take steps to prevent becoming a victim, just as you lock the doors to your home, office, and automobile.

Should you need a solution to protect your most important information assets with a minimum of friction, ease of use, and massive flexibility, please join me for part 3 of this series, in which I will discuss how NetFoundry Networks can be seamlessly embedded in your software and networks to assist in mitigating risk. All three of these papers can be found freely available on Netfoundry.io in the “Resources” section.

Learn more with these resources:

All Papers in this series are posted here:

https://netfoundry.io/resources/#whitepapers

Web: https://netfoundry.io

Blog: https://netfoundry.io/about/blog/

Connect on Social Media:

Twitter: @NetFoundry
LinkedIn: https://www.linkedin.com/company/17955047

About the Author

Mike Gorman, Head of Security and Compliance, NetFoundry

Mike is a seasoned Network and Security Engineer and applies his decades of experience as the Head of Security and Compliance for NetFoundry. Mike designs and manages NetFoundry's Security and Compliance program (including SOC-2 reporting) to ensure NetFoundry operations and products are secured properly, while helping to maintain an agile and highly automated development processes. In addition, Mike is a senior member of NetFoundry's engineering team, and in this role has developed monitoring and measuring systems, cloud deployment automation and DevOps tooling. Prior to NetFoundry Mike held a variety of Security and Solution Engineering roles with IBM, and Verizon.

About NetFoundry

NetFoundry is the leader in Cloud Native Networking, enabling businesses to simply, securely and cost effectively connect distributed applications across edges, clouds and service meshes. The NetFoundry platform, delivered as NaaS, enables businesses to connect applications without the costs and complexity of VPNs, custom hardware, and private circuits. NetFoundry's platform is accessed via APIs, SDKs, and DevOps tools integrations, enabling practitioners, application developers, and network administrators to get the levels of automation and agility which are only possible with connectivity-as-code.

*Disclaimer:
The information provided in this paper is offered "as-is", and is provided for general information purposes only. All information is provided in good faith. We make no representation or warranty of any kind, expressed, or implied in any way regarding the accuracy, adequacy, validity, availability or completeness of any information contained in the paper.